UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A 2TB Hitachi Hard Drive Serial Number YFGNBBTA and Labeled HD-2

Case No. 1:18mj307

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Electronic device more fully described in Attachment A, attached hereto and made a part hereof.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of, instrumentalities used in committing, and fruits of the crime of 18 U.S.C. §§ 2252A(a)(5)(B), which are more particularly described in Attachment B, attached hereto and made a part hereof.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Charles N. Cook II, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/04/18

Judge's signature

City and state: Greensboro, North Carolina

L. Patrick Auld United States Magistrate Judge
Printed name and title

ATTACHMENT A

ITEM TO BE SEARCHED

The device to be searched is related to the investigation of Timothy Donovan Burns and is in the custody of the North Carolina State Bureau of Investigation at 501 Industrial Blvd., Greensboro, North Carolina. The device is a 2TB Hitachi hard drive serial number YFGNBBTA and labeled HD-2.

ATTACHMENT B

ITEM TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, §§ 2252A(a)(5)(B).

1. For any computer or storage medium whose search is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

g. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

h. records of or information about Internet Protocol addresses used by the COMPUTER;

i. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in child exploitation content; and

2. Child pornography and child erotica.

3. Records, information, and items relating to violations of the statutes described above in the form of:

a. Records and information discussing or revealing sexual activity with or sexual interest in minors;

b. Records and information constituting or referencing communications of an illicit sexual nature with minors;

c. Records and information referencing or revealing the identity of individuals depicted in child pornography and the location depicted;

d. Records and information referencing or revealing the trafficking of child pornography and those responsible, to include records and information constituting or revealing membership or participation in groups or services that provide or make accessible child pornography and/or child erotica;

e. Records and information revealing the use of Freenet peer-to-peer network; and

f. Records and information revealing the use and identification of remote computing services such as email accounts or cloud storage where files may be stored.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form

(such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Charles N. Cook II, a Special Agent (SA) with Homeland Security Investigations (HSI) being duly sworn, depose and state as follows:

INTRODUCTION

1. I submit this affidavit in support of an application for a warrant to search a hard drive belonging to Timothy Donovan BURNS, specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2252A(a)(5)(B), which are more specifically described in Attachment B.

2. The statements in this affidavit are based in part on my own investigation as well as information provided to me by North Carolina State Bureau of Investigation (SBI) SA Rodney White and other assisting HSI investigators. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of a violation of Title 18 U.S.C. § 2252A(a)(5)(B) are presently located within the item specifically described in Attachment A.

AFFIANT EXPERIENCE & TRAINING

3. I am a Special Agent (SA) of the Department of Homeland Security (DHS), Homeland Security Investigations (HSI), and have been since November of 2005. My initial training consisted of a twenty-four-week basic academy at the Federal Law Enforcement Training Center (FLETC) during which I received instruction on various aspects of federal investigations, including child exploitation and other investigative disciplines. I am currently assigned to the Resident Agent in Charge (RAC) Winston-Salem office. I previously worked in law enforcement with the United States Customs Service for fourteen years enforcing United States import laws and regulations. I have been the case agent or supporting agent in numerous investigations, including investigations involving the production, distribution, and possession of child pornography. I have received training in the area of child pornography and child exploitation, and have observed numerous examples of child pornography, as defined in Title 18 U.S.C. § 2256. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including Title 18 U.S.C. §§ 2252A, and I am authorized by law to request a search warrant.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched, described in Attachment A, and hereinafter referred to as "the Subject Device," is as follows: One Hitachi 2TB hard drive with serial number YFGNBBTA and labeled "HD-2". The Subject Device is currently in SBI custody at the SBI Greensboro office at 501 Industrial Blvd., Greensboro, North Carolina.

STATUTORY AUTHORITY

5. This investigation concerns violations of the following statute:

a. Title 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this affidavit and Attachment B:

a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production

of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

c. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

e. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

f. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones ("cell phones") and devices. *See* 18 U.S.C. § 1030(e)(1).

g. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and

connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data

to make it inaccessible or unusable, as well as reverse the process to restore it.

j. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

PROBABLE CAUSE

7. In January 2018, SBI SA Rodney White observed that an individual using IP address 174.111.32.203 was likely interacting with child pornography via a peer-to-peer network, Freenet. SBI subpoenaed the Internet service provider and learned that the IP address resolved to "Don Burns" at an apartment located at 1402 Claxton Ridge Drive, Kernersville, North Carolina.

8. On March 14, 2018, SA White and I conducted a consensual interview ("knock and talk") with Timothy Donovan BURNS at his Kernersville apartment. We knocked on BURNS's door and were granted permission to enter the apartment. We were dressed in civilian attire and identified ourselves with credentials at the doorway. We stepped inside the front door into a living room where BURNS cleared a couch of various items so that we could have a seat. BURNS informed us that he lived alone and had

worked as a computer programmer. We advised him that we were present concerning a subject who was using the Freenet peer-to-peer network. BURNS stated that he used this network. During our conversation, BURNS admitted that he obtained child pornography using Freenet. He claimed that he did not upload any child pornography to the Internet and did not trade or sell any child pornography images. BURNS advised that file sharing programs, like BitTorrent, were too complicated and may allow law enforcement to locate him.

9. When we asked BURNS what type of images and age range he preferred, he stated fifteen to sixteen year olds. Throughout the conversation, BURNS answered our questions and then, sometimes, added a statement such as "I'm not saying I did it" with a grin. We observed numerous hard drives throughout the living room and asked BURNS which hard drive would contain the material we were looking for. BURNS then identified the Subject Device, the second hard drive in his Sentry desktop computer located on the desk in the living room. BURNS claimed he "mounted" the Subject Drive each time he used it to download. He told us his computer system did not have encryption activated.

10. BURNS gave SA White written consent for an off-site preview of his computers, which included, but was not limited to the Subject Device. SA

White provided BURNS with his business card for any questions and we left the apartment with the computers.

11. On March 20, 2018, SA White began a forensic examination of BURNS's Sentry desktop computer and observed that it contained three hard drives (HD-1, the Subject Device or HD-2, and HD-3). SA White created a forensic image of HD-1 and examined it for child pornography. SA White observed thirty-six child pornography images in the unallocated space[1] of the drive. The following is a description of two of the images:

00001327_Unallocated Clusters_FO-1207700738_PS-89174646+258.jpg: This file depicts an approximately three to four year old female nude from the waist down. The child is positioned on her back with her legs up and spread apart displaying her vagina.

00001308_Unallocated Clusters_FO-1207483286_PS-89174221+406.jpg: This file depicts an approximately two to three year old female with no clothing. The child is positioned on her back with her

[1]Unallocated clusters (also referred to as unallocated space or free space) are the available disk storage space that is not allocated to file storage. Unallocated clusters can contain deleted files or remnants of deleted files created by the Operating System and/or computer users.

legs spread in the air and her hands grabbing her ankles. The child's vagina is clearly exposed.

12. SA White created a forensic image of the Subject Device but was unable to review the data. He determined that the Subject Device was encrypted with VeraCrypt.

13. On March 20, 2018, SA White and I returned to BURNS's apartment and conducted an additional consensual interview. We asked BURNS for the password to the Subject Device. BURNS refused to provide the password. Upon further conversation, BURNS advised us that there was child pornography on the Subject Device and he didn't see how providing the password would help him.

14. HSI now plans to use tools and techniques to break the encrypted password on the Subject Device so that a search of it can be performed. While BURNS provided consent to take and search his devices, he subsequently refused to provide the password to the Subject Device, thus, I seek this search warrant for the Subject Device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly,

things that have been viewed via the Internet are typically stored for some period of time on electronic devices. I know that electronic files, or remnants of such files, can be recovered months or even years after they have been downloaded onto a storage medium or electronic device, deleted, or viewed via the Internet. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file does not actually disappear; rather, the data remains on the storage medium or electronic device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in unallocated or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten.

16. As described in Attachment B, this application requests permission to locate not only electronically stored information that might serve as direct evidence of the federal criminal statutes cited herein, but also forensic electronic evidence that establishes how the item described in Attachment A was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the item described in Attachment A because:

a. Data on a computer or electronic device can provide evidence of a file that was once on the electronic device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing document).

b. Forensic evidence on an electronic storage device can indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on an electronic device that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how an electronic device works.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how an electronic device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device.

17. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the item described in Attachment A consistent with the warrant. The examination will require authorities to use tools and techniques to break the encryption password and may require authorities to employ techniques, including but not limited to computer-assisted scans of the items, that might expose many parts of the items to human inspection in order to determine whether they contain evidence as described by the warrant. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

18. Based on the foregoing, I submit that there is probable cause to believe that the federal criminal statute cited herein has been violated, and that the contraband, property, evidence, fruits and instrumentalities of the offense, more fully described in Attachment B, are located within the item described in Attachment A. I respectfully request that this Court issue a search warrant, for the item described in Attachment A, authorizing the search for and seizure of the materials described in Attachment B.

Charles N. Cook II
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 4th day of October 2018.

L. Patrick Auld
United States Magistrate Judge
Middle District of North Carolina